Evaluación de software para entidades de certificación*[1]

[Software evaluation for Certification Authorities]

Tany VILLALBA VILLALBA[2], Orlando Clemente IPARRAGUIRRE VILLANUEVA[3]

Recibo: 20.02.2014 – Aprobación: 14.08.2014

Resumen

Existen varias soluciones de software que pueden gestionar certificados digitales y ser utilizadas por Entidad de Certificación, por lo que es útil identificar un software con la mayor funcionalidad posible, para ser adecuado y ampliado, y así conseguir una total funcionalidad de una entidad. Este software puede ser libre o propietario pero, para un mayor control y por la problemática, se sugiere que sea libre y de código abierto, de manera que puedan realizarse ajustes para adaptarse a la normatividad específica, peruana en este caso. En el análisis de este tipo de software, se usan criterios de estandarización (RFC 3647), escalabilidad, facilidad de mantenimiento y soporte por parte de empresa o comunidad de usuarios. De la comparación realizada entre soluciones, se concluye que EJBCA es la más completa, así como la de mayor facilidad de adecuación.

Palabras Clave: *certificado digital, entidad de certificación, software libre*

---

* **Modelo para la citación de este artículo**:
VILLALBA VILLALBA, Tany & IPARRAGUIRRE VILLANUEVA, Orlando Clemente (2014). Evaluación de software para Entidades de Certificación. En: Ventana Informática No. 31 (jul-dic). Manizales (Colombia): Facultad de Ciencias e Ingeniería, Universidad de Manizales. p. 91-102. ISSN: 0123-9678

1 Artículo de investigación científica y tecnológica proveniente del proyecto *Construyendo una Entidad de Certificación utilizando software Libre*, ejecutado en el periodo *02.2011-02.2013*, e inscrito en el grupo de investigación de la *Facultad de Ingeniería, Escuela Profesional de Ingeniería de Sistemas, Universidad Católica Los Ángeles de Chimbote.*

2 Ingeniero Informático y de Sistemas, MSc. en Telecomunicaciones, Especialista en Firmas Digitales, Estudiante de Doctorado en Ingeniería de Sistemas. Jefe de ECERNEP, Registro Nacional de Identificación y Estado Civil - Reniec (Lima, Perú). Correo electrónico: tanyvillalbav@gmail.com

3 Ingeniero de Sistemas, MSc. en Tecnologías de Información y Comunicaciones. Docente Titular en la Facultad de Ingeniería, Universidad Católica Los Ángeles de Chimbote (Nuevo Chimbote, Ancash, Perú). Correo electrónico: ivoc_ip@hotmail.com

Abstract

There are several software solutions for managing digital certificates and be used by Certification Body,

There are several software solutions for managing digital certificates, and be use by Certification Authority, so it is useful to identify software with maximum functionality, and extended to be suitable, and thus achieve full functionality of an entity. This software can be free or owner but, for better control and problematic, it is suggested that free and open source, so that adjustments can be made to suit the specific regulations, in this case Peruvian law code. In the analysis of this type of software, standardization criteria (RFC 3647), scalability, ease of maintenance and support from company or user community are used. From the comparison between solutions, we conclude that EJBCA is the most comprehensive, as well as the ease of adaptation.

Keywords*: digital certificate, certification authority, free software*

Introducción

Los certificados digitales, señala Talens-Oliag (2003, 1), son el equivalente a un documento de identidad, que permite a una persona demostrar que es quien dice ser, es decir que está en posesión de la clave secreta asociada a su certificado. Ellos tienen dos funciones básicas:

- Certificar que las personas, el sitio web, así como los recursos de la red (tales como servidores y *routers*), son fuentes confiables, es decir, que corresponden a lo que dicen ser.
- Brindar protección a los datos intercambiados por parte del visitante y el sitio web de la manipulación o incluso el robo, tales como información de tarjetas de crédito.

Para contar con un certificado digital se requiere de la acción de una Entidad de Certificación, y para la implementación de una entidad de certificación se requiere el uso software especializado. Normalmente, el software utilizado por las entidades de certificación tiene un alto costo de implementación por ser especializado, de poca difusión y ajustable a los requerimientos específicos de cada país.

Lo anterior, no evita que pequeñas instituciones puedan usar esta tecnología a su interior, lo cual implica contar con una entidad de certificación y un software para la emisión de certificados digitales, por lo cual se pretende evaluar y sugerir una solución libre utilizable sin impedimento de costo o conocimiento.

A pesar de existir algunas soluciones de software que pueden permitir la implementación de una entidad de certificación, varias de ellas están en desarrollo o atienden únicamente una parte del funcionamiento esperado, situación que origina el presente trabajo en busca de orientar la implementación de una entidad de certificación utilizando Software Libre, bajo el alcance del reglamento de la Ley de Firmas y Certificados Digitales en el Estado Peruano (Presidencia de la República, 2008, 12).

1. Fundamento teórico

1.1 Autoridad de Certificación o Entidad de Certificación (EC)

Es la entidad que valida certificados digitales para los usuarios finales, los cuales se usan como las identidades digitales en las transacciones electrónicas (autenticación de firmas digitales y cualquier proceso electrónico que requiera garantizar la identidad del usuario), de acuerdo con Kaushik (2007).

La Entidad de Certificación tiene un subcomponente tecnológico denominado Planta de Certificación digital o Planta PKI, correspondiente a un Centro de Datos. El software, asegura Reniec (2012a, 5), es uno de los componentes tecnológicos más importantes, ya que la generación de la identidad digital (certificado digital) es el primer paso para los temas como gobierno electrónico o cualquier modelo que requiera garantizar la autenticidad del usuario.

1.2 Certificado digital

Según Reniec (2012b), es un documento digital emitido por una entidad autorizada o Entidad de Certificación (EC), que vincula un par de claves[4] (una pública y otra privada) con una persona y asegura su identidad digital, de manera que la persona pueda ejecutar acciones de comercio y gobierno electrónico con seguridad, confianza y pleno valor legal. Las claves vinculadas son:

- Clave Privada. La posee únicamente su dueño y si se sospecha que ha caído en manos ajenas, inmediatamente debe notificarse al certificador su revocación, logrando con ello caducar su validez. Para protegerla no debe guardarse en ningún ordenador o medio de almacenamiento, ni ser expuesta a otras personas.

4 Estas dos claves tiene una relación matemática única que funcionan a manera de llave y contra-llave, así lo que cifre la clave privada exclusivamentemente puede ser decifrada por la clave pública y viceversa.

- Clave Pública. Llamada también parte pública, puede ser publicada en la web por la autoridad de Certificación después de ser aprobada por ella, como consta el RFC 3647, sin embargo, basta con certificar su validez. Asimismo, esta clave será conocida por todas las personas con quienes se relacione.

Un certificado digital puede ser utilizado para identificar una persona, identificar un equipo servidor, un medio de validación para sistemas de acceso como puertas o bibliotecas, entre otras utilidades. Los certificados digitales se basan en la criptografía de clave pública que utiliza el par de claves descritas para cifrado y el descifrado. Con la criptografía de la clave pública, las llaves o claves (*key*)[5] funcionan en pares emparejados de público y privado.

1.3 Software para Certificación Digital

Para implementar una Entidad de Certificación Digital, se tienen varias opciones de software en temas de PKI (*Public Key Infrastructure*), como:

- Portecle: una aplicación con interfaz gráfica fácil de usar para la creación, la gestión y el examen de los almacenes de claves.
- XCA-X: aplicación diseñada para crear y gestionar certificados X.509, solicitudes de certificados, RSA, DSA y CE claves privadas, tarjetas inteligentes y las CRL. Con ella, las entidades pueden firmar subCA de forma recursiva de forma fácil, además hay plantillas personalizables que se pueden utilizar para la generación del certificado digital.
- EJBCA-PKI: según EJBCA (2014), permite construir una infraestructura completa (o varios) en una instancia de EJBCA, tiene un número ilimitado de entidades emisoras de certificados raíz y SubCA, solicitud de certificados y certificados cruzados de puentes de otras entidades emisoras de certificados y Puente de las CA. Además, permite certificados cruzados a otras CA.
- Win-PCA: Sourceforce (2010), señala que es un script para crear infraestructura de certificados autofirmado de raíz.
- OpenCA Labs: se basa en muchos proyectos de Código Abierto. Según OpenCA (2011), entre el software necesario está OpenLDAP, OpenSSL, Apache Proyecto, Apache mod_ssl. El desarrollo del proyecto se divide en dos tareas principales: estudiar y perfeccionar el sistema de seguridad que garantiza el mejor modelo para ser

5 En sistemas criptográficos, señala Entrust (2007), el término *key* se refiere a un valor numérico que se utiliza un algoritmo para alterar la información segura y visible solo para las personas que tienen la clave correspondiente para recuperar la información.

utilizado en una CA y el desarrollo de software para configurar y administrar fácilmente una Autoridad de Certificación.

- OpenSSL: se basa en la biblioteca SSLeay desarrollada por Eric A. Young y Tim J. Hudson. El *kit* de herramientas OpenSSL está bajo una licencia de tipo Apache, lo que implica la libertad de obtenerlo y utilizarlo para fines comerciales y no comerciales, con sujeción a ciertas condiciones de licencia simples, indica OpenSSL (2013). Esta aplicación, a pesar de las múltiples críticas sobre la baja calidad del código heredado de SSLeay, particularmente su falta de limpieza, como en el caso de *Heartbleed*, es usada como biblioteca base de desarrollo, por ser un software de tipo línea de comando al cual se le puede implementar *script* para automatizar algunas tareas manuales convirtiéndolo en una posible solución para ser utilizada por una Entidad de Certificación.

Debe aclararse que la emisión de certificados digitales usados para cifrado de datos, tiene un ámbito regulatorio restrictivo según el reglamento de la Ley Peruana de Firmas y Certificados Digitales (Presidencia de la República, 2008, 12), por lo cual no se abarca en el presente trabajo.

1.4 Referencias

Uno de los referentes más grandes son los estudios realizados por la RNP (*Red Nacional de Ensino e Pesquisa - Brasil*) a través de la Escuela Superior de Redes (Carlos et al., 2010), quienes publicaron un libro que contempla de forma íntegra y didáctica la implementación de una entidad de certificación partiendo de lo básico y llega al nivel de detalle técnico, utilizando apenas una herramienta de software como OpenSSL.

Otro gran centro de investigación sobre entidades de certificación y gobierno electrónico a través de numerosas tesis y proyectos de investigación es LabSEC (*Laboratório de Segurança em Computação*), de la Universidad Federal de Santa Catarina - Brasil, con proyectos como Sistema Gerenciador de Certificados (LabSEC, 2013), el cual implementa una entidad de certificación desde cero.

2. Metodología

La metodología utilizada fue el modelo de tecnología aplicada, debido a que se propone resolver e implementar (caso práctico) cuestiones que surgen de la necesidad de desarrollar un proceso con eficacia. Conceptualmente, la característica principal de la investigación aplicada tecnológica fue utilizada para resolver problemas prácticos, no pretende descubrir ni explicar los hechos reales, sino transformarlos o

adecuarlos en el sentido más práctico para plantear una alternativa de solución viable y pertinente al problema.

Por lo expuesto, para llegar a un resultado (la elección de un software adecuado) fue necesario instalar cada software y simular un entorno de producción, para comprobar sus funcionalidades contra una lista de cumplimiento (RFC 3647 *checklist*), como mecanismo de comparación.

3. Resultados y discusión

Para la evaluación de aplicaciones utilizables en Entidades de Certificación, se partió de un listado de 13 opciones (Tabla 1), conformado por lo más populares con licencia gratuita y de preferencia con código abierto.

Tabla 1. Listado de software consideradas para Entidades de Certificación

#	Nombre del software	URL	Licencia
1	Portecle v1.7	http://portecle.sourceforge.net/	GNU General Public License (GPL)
2	XCA v.0.9.3	http://xca.sourceforge.net/	BSD License
3	EJBCA v.4.0.9	http://www.ejbca.org/	GNU Library or Lesser General Public License (LGPL)
4	Win PCA v.0.1	http://win-pca.sourceforge.net/	Apache License V2.0
5	OpenCA v.1.1.0	www.openca.org/	BSD License
6	CA Web Helper v.1.1	cawh.sf.net	GNU General Public License (GPL)
7	PHPki v.0.83	http://phpki.sourceforge.net/	GNU General Public License (GPL)
8	CertForge v.1.1	certforge.sf.net	GNU General Public License (GPL)
9	myca.sf.net v.0.1	My Certificate Authority Shell	GNU General Public License (GPL)
10	pkIRIS v.0.8	http://www.rediris.es/app/pkiris	GNU General Public License (GPL)
11	Open SSL v.0.98	http://www.openssl.org/	Especificaciones propias
12	SITIv.1.0	https://projetos.labsec.ufsc.br/siti	Especificaciones propias
13	NewPKI v.2.0	http://www.newpki.com	GNU General Public License (GPL)

En cada uno de ellos, se consideraron dos requerimientos obligatorios para que un software pueda utilizarse por una entidad de certificación:

Ley de Firma y Certificados Digitales, en caso de tratarse de Gobiernos o Normas internas en caso de instituciones pequeñas, ya que la Entidad de Certificación se implementa de acuerdo con los requerimientos internos a manera de declaraciones de cumplimiento, debido a que ellos puede ser variables (al estar en función de las leyes nacionales), por lo que no es un criterio especifico de evaluación para el software.

RFC 3647 (*Request for Comments*). Chokhani et al. (2003, 1), especifica los ítems referentes al despliegue de una Entidad o Autoridad Certificadora tecnológicamente hablando (Tabla 2), que deben ser cumplidos obligatoriamente por cualquier tipo de software usado por ella.

Los valores, de la Tabla 2, se obtuvieron en las pruebas a cada software, bien desde la instalación realizada o desde uso de versiones *life* disponibles en la respectiva página web. En el caso de ítems exigidos no demostrables como parte del uso de software, se tomó como referencia la documentación presentada en la página web correspondiente, donde se declara su cumplimiento, mientras se consignó como Falta de Información (Fi) cuando no se pudo obtener información de su página web ni del aplicativo software.

Tabla 2. Análisis de cumplimiento de estándares técnicos y legales (construida a partir de Chokhani et al., 2003, 1)

Sección	Subsección	Software						
		XCA	Portecle	EJBCA	OpenCA	OpenSSL	SITI	New pki
1. Introducción	1.2 Nombre e identificación del documento.	Sí	No	Sí	Sí	Ma	No	Fi
	1.3.1 Entidades de certificación	Sí	No	Sí	Sí	Ma	Sí	Sí
	1.4 Uso del certificado	Sí	No	Sí	Sí	Ma	Sí	Sí
2. Publicación y responsabilidades del repositorio	2.1 Repositorios	No	No	Sí	Sí	Ma	No	Sí
	2.2 Publicación de la información sobre certificación	Fi	No	Sí	Sí	Ma	Sí	No
	2.3 Tiempo o frecuencia de la publicación	Fi	No	Sí	Ma	Ma	Ma	Ma
	2.4 Controles de acceso a los repositorios	No	No	Sí	Sí	Ma	Sí	Sí
3. Identificación y autenticación	3.1.1 Tipos de nombres	Sí	No	Sí	Sí	Ma	Sí	Sí
	3.2.1 Método para probar la posesión de la clave privada	Sí	No	Fi	Fi	Ma	Fi	Fi
	3.4 Identificación y autenticación de la solicitud de revocación	No	No	Sí	Sí	Ma	Sí	No

Si = soporta
No = no soporta
Ma = Manual
Fi = Falta información

Sección	Subsección	Software						
		XCA	Portecle	EJBCA	OpenCA	OpenSSL	SITI	New pki
4. Requisitos operacionales del Ciclo de vida de los Certificado	4.2.2 Aprobación o rechazo de la solicitud de emisión de un certificados	No	No	Sí	Sí	Ma	Sí	Sí
	4.2.3 Tiempo para el procesamiento de la solicitud de un certificado							
	4.3.1 Acciones de la EC durante la emisión del certificado	Sí	No	Sí	Sí	Ma	Sí	Sí
	4.3.2 Notificación al suscriptor por parte de la EC respecto de la emisión de un certificado	No	No	Fi	Fi	Ma	No	No
	4.4.1 Conducta constitutiva de la aceptación de un certificado	No	No	Fi	Fi	Ma	Fi	Fi
	4.4.2 Publicación del certificado por parte de la EC	No	No	Si	Si	Ma	Si	Si
	4.7 Re-emisión de certificado. Sólo se aplica a seguridad media alta. (opcional)	No	No	Fi	Fi	Ma	No	No
	4.7.1 Circunstancias para la re-emisión de un certificado	No	No	Fi	Fi	Ma	No	No
	4.7.4 Notificación al suscriptor sobre la re-emisión de un certificado	No	No	Fi	Fi	Ma	No	No
	4.8 Modificación del certificado (opcional)	No	No	No	No	Ma	No	No
	4.8.4 Notificación al suscriptor sobre la emisión de un nuevo certificado	No	No	Fi	Fi	Ma	Fi	Fi
	4.9.3 Procedimiento para la solicitud de revocación	No	No	Sí	Sí	Ma	Sí	Sí
	4.9.5 Tiempo dentro del cual una EC debe procesar la solicitud de revocación	Ma	No	Ma	Ma	Ma	Ma	Ma
	4.9.7 Frecuencia de emisión de CRL [lista de revocaciones de certificados]	Ma	No	Si	Si	Ma	Ma	Ma
	4.9.8 Máxima latencia para CRL	Ma	No	Ma	Ma	Ma	Ma	Ma
	4.9.9 Disponibilidad de la verificación en línea de la revocación/estado	No	No	Si	Si	Ma	No	No
	4.9.13 Circunstancias para la suspensión	Fi	No	Fi	Fi	Ma	No	No
	4.10.3 Rasgos operacionales	No	No	Sí	Sí	Ma	No	No
	4.12.1 Políticas y prácticas de recuperación de Depósito de claves	Sí	No	Sí	Sí	Ma	Sí	Sí
	4.12.2 Políticas y prácticas para la encapsulación de claves de sesión	No	No	Si	Ma	Ma	No	No

Sección	Subsección	Software						
		XCA	Portecle	EJBCA	OpenCA	OpenSSL	SITI	New pki
5. Controles de instalaciones, de gestión y operacionales	5.4. Procedimiento de registro de auditoría 5.4.1 Tipos de eventos registrados	No	No	Sí	Sí	Ma	Sí	Sí
	5.4.2 Frecuencia del procesamiento del registro	No	No	Sí	Sí	Ma	No	No
6. Controles de Seguridad Técnica	6.1 Generación e instalación del par de clave 6.1.5 Tamaño de las claves	Sí	Sí	Sí	No	Ma	No	No
	6.2 Controles de ingeniería para protección de la clave privada y módulo criptográfico	Fi	No	Sí	Fi	Ma	Fi	Fi
	6.2.3 Depósito de clave privada 6.2.7 Almacenamiento de la clave privada en un módulo criptográfico	Fi	No	Si	Si	Ma	No	No
	6.6 Controles técnicos del ciclo de vida 6.6.2 Controles de gestión de seguridad	No	No	Sí	Sí	Ma	Sí	Sí
7. Perfiles de Certificado	7.1 Perfil de certificado	Sí	No	Sí	Sí	Ma	Sí	Sí
	7.1.1 Número(s) de versión(es)	Si	No	Fi	Fi	Ma	Fi	Fi
	7.1.2 Extensiones del certificado	Fi	No	Si	Si	Ma	Si	Si
	7.1.3 Identificadores de Objeto de algoritmo	Fi	No	Si	Si	Ma	Si	Si
	7.1.4 Forma de nombres	Fi	No	Si	Si	Ma	Si	Si
	7.1.5 Restricciones de nombre	Fi	No	Si	Si	Ma	Si	Si
	7.1.6 Identificador de objeto de la política de certificados	Fi	No	Si	Si	Ma	Si	Si
	7.1.7 Extensión de restricciones de uso de la política	Fi	No	Si	Si	Ma	Si	Si
	7.1.8 Sintaxis y semántica de los calificadores de la política	Fi	No	Si	Si	Ma	Si	Si
	7.1.9 Procesamiento de semántica para la extensión de políticas de certificados críticos	Fi	No	Si	Si	Ma	Si	Si
	7.2 Perfil CR 7.2.1 Número(s) de versión(es)	Fi	No	Sí	Sí	Ma	Sí	Sí
	7.2.2 CRL y Extensiones de entrada de CRL	Fi	No	Si	Si	Ma	Si	Si
	7.3 Perfil OCSP	Fi	No	Sí	Sí	Ma	Sí	Sí
	7.3.1 Número(s) de versión(es)	Fi	No	Si	Si	Ma	Si	Si
	7.3.2 Extensiones OCSP	No	No	Si	Si	Ma	Si	Si

3.1 Descripción de resultados

Como se muestra en la figura 1, ningún software listado tiene un cumplimiento de los requerimientos al 100% del estándar RFC 3647. De 52 puntos evaluados el cumplimiento (Sí) fue: *XCA 10*, *Portecle 1*, *EJBCA 38*, *OpenCA 34*, *Openssl 0*, *Siti 27*, *NewPKI 27*. Como se observa el software que presenta mayor cantidad de ítems cumplidos es EJBCA y por sus características técnicas (lenguaje, soporte, tiempo de vida del proyecto, comunidad que lo respalda) hace que sea el más adecuado para realizar futuros test, adecuaciones necesarias y despliegue posterior.

Por ser el software elegido de tipo libre, se hace necesario que tenga una comunidad activa o que exista una empresa dando soporte en caso de presentar inconvenientes, que en el caso de EJBCA es activa, siendo posible encontrar apoyo para enfrentar situaciones como los problemas de codificación o *bug*. Otro punto importante es que está elaborado en lenguaje de programación java, un lenguaje popular y difundido, lo cual facilita la ubicación de personas conocedores en esta plataforma.

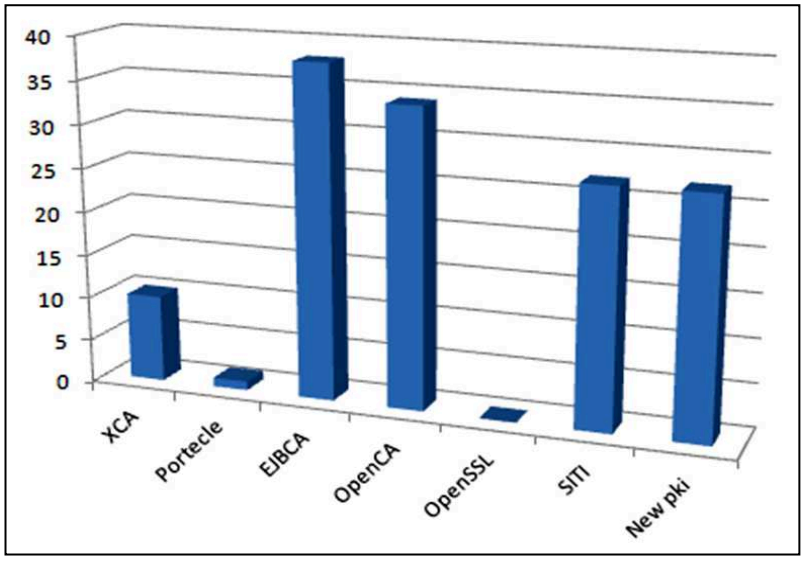

Figura 1. Cumplimiento de estándar RFC 3647 en las aplicaciones evaluadas

3.2 Discusión de resultados

Adicionalmente, al software EJBCA se le encontraron ventajas técnicas que servirán para integración y mayor alcance al requerido, como son:

- Acceso a sus opciones de manejo a través de *webservices*.
- Puede ser desplegado en cualquier sistema operativo de servidor.

- Tiene documentación en la web y una comunidad activa.
- Usa estándares de desarrollo como ejb, *framework* de persistencia y MVC, entre otros.
- Un punto a realzar, es que la integración con hardware especializado de criptografía suministra un alcance mucho mayor a plataformas de entidades de certificación, aspecto crucial en la elección del software, debido a que el desarrollo de módulos de integración con hardware especializado es complicado y el tiempo de desarrollo como la curva de aprendizaje son altos[6].
- Adicionalmente cuenta con un pequeño módulo de software de entidad de registro para probar y dar una idea de cómo debería ser el despliegue de un software de este tipo.

En la Figura 1, se aprecia que OpenCA (la siguiente opción posible) no cuenta con algunas características técnicas: lenguaje contemporáneo, *webservice* de acceso alterno, modelo fácilmente escalable, documentación suficiente para incrementar funcionalidades como la de unir a un equipo criptográfico (HSM).

4. Conclusiones

El software EJBCA es el más atractivo para ser utilizado y adecuado a las necesidades requeridas. Por presentar la mayor cantidad de puntos exigidos por el estándar RFC 3647 (marco tecnológico mínimo para una Entidad de Certificación). Además de que está construido en un lenguaje popular y extendido, como es Java, que cuenta con una comunidad activa que puede dar respaldo y soporte en caso de requerirse.

Las opciones de software examinadas son aptas para la emisión de certificados digitales, pero muchos de ellas no tiene funcionalidades completas o cumplen requisitos mínimos, que pueden ser utilizados para sub-tareas muy especializadas, como por ejemplo únicamente emitir certificados digitales para ser usados en conexiones seguras o cifrado de canales o para autenticación de sistemas de software.

El software EJBCA, actualmente viene siendo utilizado por otras entidades de certificación en el ámbito mundial, lo que le da mayor respaldo y seriedad, además de ser respaldadas por otras empresas para su desarrollo continuo.

6 La integración con hardware criptográfico debe tomarse con especial cuidado, partiendo de un equipo comprobadamente seguro, para evitar situaciones anómalas, como aquella donde al recolector de entropía para generación de números aleatorios reales en chips Intel, y en proyectos orientados a la seguridad, como OpenBSD, lo han deshabilitado por dudar de que pueda estar intervenido por la NSA (*National Security Agency*).

Referencias bibliográficas

CARLOS, Marcelo Carlomagno; SUTIL, Jeandré Monteiro; MOECKE, Cristian Thiago & KOHLER, Jonathan Gehard (2010). Introdução a Infraestrutura de Chaves Públicas e Aplicações [Online]. Projetos especiais. Cuiabá (Mato Grosso, Brasil): Escola Superior de Redes RNP. 216 p. [Creative Commons: Atribuição e Uso Não-Comercial 2.5 Brasil]. <http://esr.rnp.br/publicacoes/seguranca/icpedu?download=44f683a84163b3523afe57c2e008bc8c> [consulta: 09/03/2014]

CERTIFICADO DIGITAL (2000). Certificado Digital: Guía del usuario, Versión 1.0 [en línea]. Buenos Aires (Argentina): Certificado Digital S.A. 17 p. <http://www.certificadodigital.com.ar/download/GUsuario.pdf> [consulta: 22/04/2014]

CHOKHANI, S.; FORD, W.; SABETT, R.; MERRILL, C. & WU, S. (2003). Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [online]. Fremont (California, USA): IETF Working Groups. 94 p. <http://www.ietf.org/rfc/rfc3647.txt> [consult: 09/03/2014].

EJBCA (2014). EJBCA PKI by PrimKey: Reference installations [online]. Solna (Sweden): PrimeKey Solutions AB (Last published: 07/04/2014). <http://www.ejbca.org/installations.html> [consult: 28 /01/2014].

ENTRUST (2007). Securing your Digital life: Understanding Diigtal Certificates & Secure Socktes Layers [online]. Dallas (TX, USA): Entrust, Securing Digital Identifies & Information. 11 p. <http://www.entrust.net/ssl-resources/pdf/understanding_ssl.pdf> [consult: 05/01/2014].

HOHNSTÄDT, Christian (2012). XCA - X Certificate and key management [online]. Berlin (Germany). XCA. sourceforget. <http://xca.sourceforge.net> [consult: 05/01/2014].

KAUSHIK, Vivek (2007). Digital Certificate Extensions: Should "basic constraints" be marked critical? [online]. Dallas (TX, USA): Entrust, Securing Digital Identifies & Information. 4 p. <https://www.netrust.net/docs/whitepapers/BasicConstraints_whitepaper_v1.0.pdf> [consult: 05/01/2014].

LABSEC (2013). Gestão do Ciclo de Vida de Chaves Criptográficas e Certificados Digitais: Sistema Gerenciador de Certificados Versão 2.0 [Online]. Florianópolis (Santa Catarina, Brasil): Universidade Federal de Santa Catarina, Laboratório de Segurança em Computação (Última atualização: 29/08/2014). <http://www.labsec.ufsc.br/gestao-do-ciclo-de-vida-de-chaves-criptograficas-e-certificados-digitais/> [consulta: 09/03/2014].

OPENCA LABS (2011). LIPKI V0.6.5 (HOPE) [ONLINE]. MODENA (ITALY): POENCA LABS: OPENSOURCE SECURITY AND IDENTITY MANAGEMENT SOLUTIONS <HTTPS://PKI.OPENCA.ORG> [CONSULT: 10/11/2013].

OPENSSL (2013). Welcome to the OpenSSL Project [online]. Vällington (Sweden): OpenSSL SE <http://www.openssl.org/> [consulta: 12/11/2013].

PRESIDENCIA DE LA REPÚBLICA (Perú) (2008). Reglamento de la ley de firmas y certificados digitales, Decreto Supremo Nº 052-2008-PCM [en línea]. Lima (Perú): Presidencia de la República. <http://www.minjus.gob.pe/wp-content/uploads/2014/03/DS-052-2008-pcm.pdf> [consulta: 06/01/2014]

REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL, RENIEC (2012a). Planta de Certificación Digital [en línea]. Lima (Perú): Reniec. 107 p. <http://www.reniec.gob.pe/portal/pdf/02_pki.pdf> [consulta: 06/01/20014].

REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL, RENIEC (2012b). Certificado Digital [en línea]. Lima (Perú): Reniec. <http://www.reniec.gob.pe/portal/b01_bPKI.htm> [consulta: 06/01/2014].

SOURCEFORGE (2004). Portecle [online]. Fairfax County (Virginia, USA): Geeknet Inc. <http://portecle.sourceforge.net> [consult: 05/01/2014].

SOURCEFORGE (2010). Win PCA [online]. Fairfax County (Virginia, USA): Geeknet Inc. <http://sourceforge.net/projects/win-pca> <http://win-pca.sourceforge.net/> [consult: 02/12/2013].

TALENS-OLIAG, Sergio (2003). Introducción a los certificados digitales [en línea]. En: Boletín Electrónico de InfoCentre (nov.) Valencia (España): Universidad de Valencia. p. 1-5 <http://www.uv.es/~sto/articulos/BEI-2003-11/certificados_digitales.pdf> [consulta: 10/01/2014]